**РЕФЕРАТ**

по дисциплине «Информатика»

по теме: «Антивирусные программы»

**Содержание**

Компьютерные вирусы и вредоносные программы, программы борьбы с ними

Методы обнаружения вирусов

Метод соответствия определению вирусов в словаре

Метод обнаружения странного поведения программ

Другие методы обнаружения вирусов

Проблемы борьбы с вирусами

Антивирусная программа AVP

Интерфейс AVP

Тестовые примеры

Литература

**Компьютерные вирусы и вредоносные программы, программы борьбы с ними**

С увеличением количества людей, пользующихся компьютером, и возможностей обмена между ними данными по электронной почте и через интернет возросла угроза заражения компьютера вирусами, а также порчи или хищения информации прочими вредоносными программами.

В целом вредоносные программы можно разделить на следующие три класса:

* **Черви** – данная категория вредоносных программ для распространения использует сетевые ресурсы. Название этого класса было дано исходя из способности червей «переползать» с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому черви обладают исключительно высокой скоростью распространения.

Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

* **Вирусы** – программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – *заражение*. Скорость распространения вирусов несколько ниже, чем у червей.
* **Троянские программы** – программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к «зависанию», воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

В последнее время наиболее распространенными типами вредоносных программ, портящими компьютерные данные, стали черви. Далее по распространенности следуют вирусы и троянские программы. Некоторые вредоносные программы совмещают в себе характеристики двух или даже трех из перечисленных выше классов.

Основными источниками распространения вредоносных программ является электронная почта и интернет, хотя заражение может также произойти через дискету или CD-диск. Это обстоятельство предопределяет смещение акцентов антивирусной защиты с простых регулярных проверок компьютера на присутствие вирусов на более сложную задачу постоянной защиты компьютера от возможного заражения. [2]

Антивирусная программа (антивирус) предназначена для защиты компьютеров от большинства вирусов, червей и «троянских коней», которые могут удалить файлы, получить доступ к личным данным либо использовать зараженную систему как средство атаки на другие компьютеры. Антивирусная программа может быть предустановлена на компьютер, а может быть приобретена и установлена самостоятельно. [1]

Первые, наиболее простые антивирусные программы появились почти сразу после появления вирусов. Сейчас разработкой антивирусов занимаются крупные компании. Как и у создателей вирусов, в этой сфере также сформировались оригинальные приёмы — но уже для поиска и борьбы с вирусами. Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.

К сожалению, конкуренция между антивирусными компаниями привела к тому, что развитие идёт в сторону увеличения количества обнаруживаемых вирусов (прежде всего для рекламы), а не в сторону улучшения их детектирования (идеал — 100%-ое детектирование) и алгоритмов лечения заражённых файлов.

Антивирусное программное обеспечение состоит из компьютерных программ которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы. [3]

**Методы обнаружения вирусов**

Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

Просмотр (сканирование) файлов для поиска известных вирусов, соответствующих определению в словаре вирусов

Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

**Метод соответствия определению вирусов в словаре**

Это метод, когда антивирусная программа, просматривая файл, обращается к словарю с известными вирусами, который составлен авторами программы-антивируса. В случае соответствия какого либо участка кода просматриваемой программы известному коду вируса в словаре, программа антивирус может заняться выполнением одного из следующих действий:

Удалить инфицированный файл.

Отправить файл в карантин (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса).

Попытаться восстановить файл, удалив сам вирус из тела файла.

Для достижения достаточно продолжительного успеха, при использовании этого метода необходимо периодически пополнять словарь известных вирусов новыми определениями (в основном в онлайновом режиме). Обладающие чувством гражданского долга и технически искушённые пользователи, обнаружив «живьём» новый вирус, могут выслать заражённый файл разработчикам антивирусных программ, которые включат затем новый вирус в словарь.

Антивирусные программы, созданные на основе метода соответствия определению вирусов в словаре, обычно просматривают файлы тогда, когда компьютерная система создаёт, открывает, закрывает или посылает файлы по электронной почте. Таким образом, вирусы можно обнаружить сразу же после занесения их в компьютер и до того, как они смогут причинить какой-либо вред. Надо отметить, что системный администратор может составить график для антивирусной программы, согласно которому могут просматриваться (сканироваться) все файлы на жёстком диске.

Хотя антивирусные программы, созданные на основе поиска соответствия определению вируса в словаре, при обычных обстоятельствах, могут достаточно эффективно препятствовать вспышкам заражения компьютеров, авторы вирусов стараются держаться на полшага впереди таких программ-антивирусов, создавая «олигоморфические», «полиморфические» и, самые новые, «метаморфические» вирусы, в которых некоторые части шифруются или искажаются так, чтобы невозможно было обнаружить совпадение с определением в словаре вирусов.

**Метод обнаружения странного поведения программ**

Антивирусы, использующие метод обнаружения подозрительного поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается записать какие-то данные в исполняемый файл (exe-файл), программа-антивирус может пометить этот файл, предупредить пользователя и спросить что следует сделать.

В отличие от метода соответствия определению вируса в словаре, метод подозрительного поведения даёт защиту от совершенно новых вирусов, которых ещё нет ни в одном словаре вирусов. Однако, программы, построенные на этом методе, выдают также большое количество ошибочных предупреждений, что делает пользователя мало восприимчивым ко всем предупреждениям. Если пользователь нажимает мышью на окно «Принять» («Accept») в каждом случае появления такого предупреждения, антивирусная программа не приносит никакой пользы. В последнее время эта проблема ещё более ухудшилась, так как стало появляться всё больше невредоносных программ, модифицирующих другие exe-файлы, несмотря на существующую проблему ошибочных предупреждений. Таким образом, в современном антивирусном программном обеспечении этот метод используется всё меньше и меньше.

**Другие методы обнаружения вирусов**

Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы, перед тем как передать ей управление. Если программа использует самоизменяющийся код или проявляет себя как вирус (то есть немедленно начинает искать другие exe-файлы например), такая программа будет считаться вредоносной, способной заразить другие файлы. Однако этот метод тоже изобилует большим количеством ошибочных предупреждений.

Ещё один метод определения вирусов включает в себя использование «песочницы». Песочница имитирует операционную систему и запускает исполняемый файл в этой имитируемой системе. После исполнения программы, антивирусное программное обеспечение анализирует содержимое песочницы на присутствие каких либо изменений, которые можно квалифицировать как вирус. Из-за того, что быстродействие системы снижается и требуется достаточно продолжительное время для выполнения программы, антивирусные программы, построенные по этому методу, обычно используются только для сканирования по запросу пользователя. Следует отметить, что эффективность данных программ намного выше, чем у всех остальных, но и стоимость их тоже выше. Из-за большого времени таких выполнения программ, они не найдут широкого распространения среди рядовых пользователей. Несомненно, эти программы представляют интерес для профессионалов, занимающихся вопросами компьютерной безопасности и восстановлением данных после несанкционированного доступа в компьютер пользователя или атак на сервер.

**Проблемы борьбы с вирусами**

Распространение вирусов по электронной почте (возможно наиболее многочисленных и вредоносных) можно было бы предотвратить недорогими и эффективными средствами без установки антивирусных программ, если бы были устранены дефекты программ электронной почты, которые сводятся к выполнению без ведома и разрешения пользователя исполняемого кода, содержащегося в письмах.

Обучение пользователей может стать эффективным дополнением к антивирусному программному обеспечению. Простое обучение пользователей правилам безопасного использования компьютера (например не загружать и не запускать на выполнение неизвестные программы из Интернета) снизило бы вероятность распространения вирусов и избавило бы от надобности пользоваться многими антивирусными программами.

Пользователи компьютеров не должны всё время работать с правами администратора. Если бы они пользовались режимом доступа обычного пользователя, то некоторые разновидности вирусов не смогли бы распространяться (или, по крайней мере, ущерб от действия вирусов был бы меньше). Это одна из причин, по которым вирусы в Unix-подобных системах относительно редкое явление.

Метод обнаружения вирусов по поиску соответствия в словаре не всегда достаточен из-за продолжающегося создания всё новых вирусов, метод подозрительного поведения не работает достаточно хорошо из-за большого числа ошибочных решений о принадлежности к вирусам незаражённых программ. Следовательно, антивирусное программное обеспечение в его современном виде никогда не победит компьютерные вирусы.

Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы необнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. К несчастью, во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

Постоянное появление новых вирусов даёт разработчикам антивирусного программного обеспечения хорошую финансовую перспективу.

Некоторые антивирусные программы могут значительно понизить быстродействие. Пользователи могут запретить антивирусную защиту, чтобы предотвратить потерю быстродействия, в свою очередь, увеличивая риск заражения вирусами. Для максимальной защищённости антивирусное программное обеспечение должно быть подключено всегда, несмотря на потерю быстродействия. Некоторые антивирусные программы (как AVG for Windows) не очень сильно влияют на быстродействие.

Иногда приходиться отключить антивирусную защиту при установке обновлений программ, таких, например, как Windows Service Packs. Антивирусная программа, работающая во время установки обновлений, может стать причиной неправильной установки модификаций или полной отмене установки модификаций. Перед обновлением Windows 98, Windows 98 Second Edition или Windows ME на Windows XP (Home или Professional), лучше отключить защиту от вирусов, в противном случае процесс обновления может завершиться неудачей. [3]

**Антивирусная программа AVP**

Антивирус Касперского Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционной системы Windows.

Антивирус Касперского Personal выполняет следующие функции:

* **Защита от вирусов и вредоносных программ** – обнаружение и уничтожение вредоносных программ, проникающих через съемные и постоянные файловые носители, электронную почту и протоколы интернета. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности).
* **Постоянная защита компьютера** – проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.
* **Проверка компьютера** **по требованию** – проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку можно запускать самостоятельно или настроить ее регулярный автоматический запуск.
* **Восстановление работоспособности после вирусной атаки**. Полная проверка и лечение с рекомендуемыми экспертами Лаборатории Касперского настройками позволяет удалить все вирусы, поразившие данные при вирусной атаке.
* **Проверка и лечение входящей/исходящей почты** – анализ на присутствие вирусов и лечение входящей почты до ее поступления в почтовый ящик и исходящей почты в режиме реального времени. Кроме того, программа позволяет проверять и лечить почтовые базы различных почтовых клиентов по требованию.
* **Обновление антивирусных баз и программных модулей** – пополнение антивирусных баз информацией о новых вирусах и способах лечения зараженных ими объектов, а также обновление собственных модулей программы. Обновление выполняется с серверов обновлений Лаборатории Касперского или из локального каталога.
* **Рекомендации по настройке программы и работе с ней** – советы от экспертов Лаборатории Касперского, сопровождающие вас в процессе работы с Антивирусом Касперского Personal, и рекомендуемые настройки, соответствующие оптимальной антивирусной защите.

В случае обнаружения зараженных или возможно зараженных файлов, когда антивирусные базы не обновляются критически долгий срок, или когда давно не проводилась полная проверка компьютера, в главном окне Антивируса Касперского всегда присутствуют рекомендации по выполнению тех или иных действий и обоснования для их совершения. Сразу после установки продукта и его запуска вступают в силу рекомендуемые экспертами настройки антивирусной защиты.

* **Карантин** – помещение объектов, возможно зараженных вирусами или их модификациями, в специальное безопасное хранилище, где вы можете их лечить, удалять, восстанавливать в исходный каталог, а также отправлять экспертам Лаборатории Касперского на исследование. Файлы на карантине хранятся в специальном формате и не представляют опасности.
* **Формирование отчета** – фиксирование всех результатов работы Антивируса Касперского Personal в отчете. Подробный отчет о результатах проверки включает общую статистику по проверенным объектам, хранит настройки, с которыми была выполнена та или иная задача, а также последовательность проверки и обработки каждого объекта в отдельности. Отчет формируется и по результатам обновлений. [2]

## Интерфейс AVP

Антивирус Касперского Personal обладает достаточно простым и удобным в работе интерфейсом. Рассмотрим основные его элементы:

**1. Значок в Системной панели**

После запуска продукта в Системной панели появляется значок, вид которого зависит от состояния постоянной антивирусной защиты. Если постоянная защита файлов включена, значок активен (красного цвета), если выключена – неактивен (серого цвета), даже если выполняется проверка почты или сценариев.

Если выполняется анализ какого-либо объекта в режиме постоянной защиты, то значок располагается поверх мигающей бело-синей папки. При проверке почты вместо папки появляется конвертик.

Когда происходит важное с точки зрения антивирусной безопасности событие, на некоторое время над значком появляется информационное сообщение с рекомендацией от экспертов Лаборатории Касперского.

**2. Контекстное меню**

Если щелкнуть правой кнопкой мыши в Системной панели по значку программы, откроется контекстное меню, состоящее из следующих пунктов:

*Открыть Антивирус Касперского* – открыть главное окно программы на закладке Защита. Выполнить данное действие также можно, дважды щелкнув левой кнопкой мыши по значку программы в Системной панели.

*Проверить Мой компьютер на вирусы* – запустить полную проверку компьютера на вирусы в соответствии с установленным уровнем защиты.

*Обновить антивирусные базы* – загрузить обновления антивирусных баз с серверов обновлений Лаборатории Касперского.

*Включить постоянную защиту / Выключить постоянную защиту* – включить / отключить постоянную защиту компьютера. В зависимости от того, включена ли постоянная защита, меняется вид значка программы.

*О программе* – показать справочное окно с основными сведениями об Антивирусе Касперского Personal.

*Выход* – выгрузить Антивирус Касперского Personal из памяти компьютера. Пункт Выход контекстного меню не будет доступен, если пользователь не обладает правами администратора на компьютере.

**3. Главное окно программы**

Главное окно Антивируса Касперского Personal предназначено для реализации всех возможностей продукта по обеспечению полной антивирусной защиты компьютера. Здесь можно:

настраивать параметры антивирусной защиты;

запускать и останавливать проверки компьютера и отдельных его дисков, каталогов, файлов на присутствие вирусов и других вредоносных программ;

загружать обновления антивирусных баз и программных модулей;

настраивать автоматический запуск полной проверки и обновлений;

работать с объектами на карантине;

работать с отчетами и т.д.

Все параметры антивирусной защиты, необходимая информация и задачи сгруппированы в главном окне на следующих закладках:

*Защита* – закладка главного окна, на которой приведены задачи антивирусной защиты и их текущее состояние. Данная закладка является основным интерфейсом программы.

*Настройка* – закладка главного окна, содержащая задачи по настройке основных параметров антивирусной защиты и их текущее состояние.

*Поддержка* – закладка, включающая информацию, используемую в случае возникновения проблем или необходимости обращения за помощью в Лабораторию Касперского.

Каждая закладка делится на две части:

Левая часть закладки, содержащая гиперссылки, посредством которых реализуются задачи антивирусной защиты. Список задач зависит от назначения закладки.

Так, на закладке *Защита* приведены все возможные задачи для проверки компьютера на присутствие вирусов, на закладке Настройка – настройки параметров этих задач, на закладке Поддержка – задачи, направленные на поддержку вашей антивирусной защиты

Правая часть закладки, включающая информацию о текущем состоянии антивирусной защиты вашего компьютера (постоянной защиты, проверки по требованию и антивирусных баз, лицензионной информации).

Так, на закладке *Защита* отображается текущее состояние антивирусной защиты, на закладке Настройка – состояние ее настроек, на закладке Поддержка – статус лицензирования (информация о лицензионном ключе), ссылки на адреса поддержки, информация о программе и системе.

**4. Окно процесса проверки**

При запуске проверки компьютера или отдельных его дисков, каталогов, файлов на экране появляется окно процесса проверки.

Окно состоит из двух частей:

В верхней части расположен индикатор, отображающий выполнение процесса проверки в процентах, время начала, время предполагаемого окончания проверки, а также имя текущего проверяемого объекта.

В нижней части окна расположены три закладки:

*Статистика* – с результатами проверки,

*Отчет* – с отчетом о произошедших в процессе проверки событиях

*Настройки* – с перечнем настроек, с которыми производится проверка.

**Тестовые примеры**

**1. Обновить антивирусные базы AVP**

Щелкаем правой кнопкой мыши в Системной панели по значку программы, открывается контекстное меню AVP. Выбираем пункт «Обновить антивирусные базы». Откроется окно процесса обновления баз.

**2. Проверить на наличие вирусов файл c:\prg\test.exe**

- Запускаем Проводник.

- Переходим в папку «c:\prg».

- Щелкаем правой кнопкой мыши по файлу «test.exe», вызывая тем самым контекстное меню файла.

- Выбираем пункт «Проверить на вирусы».

- Появится окно процесса проверки.

**3. Проверить весь компьютер на наличие вирусов**

- Щелкаем правой кнопкой мыши в Системной панели по значку программы, открывается контекстное меню AVP. Выбираем пункт «Проверить Мой Компьютер на вирусы». Откроется окно процесса проверки.

В зависимости он настроек проверки по требованию, при обнаружении вируса, AVP либо запросит у пользователя, как поступить с зараженным файлом, либо удалит его, либо просто запишет информацию в отчет.

**4. Настроить автоматическую проверку всего компьютера ежедневно в 12:00**

- Щелкаем правой кнопкой мыши в Системной панели по значку программы, открывается контекстное меню AVP. Выбираем пункт «Открыть Антивирус Касперского». Откроется главное окно программы.

- Выбираем закладку «Настройка»

- Щелкаем левой кнопкой мыши по ссылке «Проверка по требованию». Откроется окно настроек:

- Щелкаем левой кнопкой мыши по ссылке «Настройка проверки по расписанию». Откроется окно:

- Выбираем настройки: проверять с интервалом в днях, запускать проверку каждый день, начало проверки – 12:00.

**5. Включить постоянную защиту компьютера с удалением зараженных объектов.**

- Открываем главное окно программы на закладке «Настройка», как указано в примере 4.

- Щелкаем левой кнопкой мыши по ссылке «Постоянная защита». Откроется окно настроек. В нем выбираем для параметра «Действия над зараженными объектами» значение «Запрещать доступ и удалять зараженные объекты»

- Щелкаем левой кнопкой мыши по ссылке «Настройка параметров защиты».

В открывшемся окне снимаем отметку с пункта «Выключить постоянную защиту», если отметка стоит.

**Литература**

1. Библиотека MSDN. http://msdn.microsoft.com

2. Руководство по программе «Антивирус Касперского»

3. Свободная энциклопедия «Википедия» http://ru.wikipedia.org